REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-33 are pending in the application. The Examiner additionally stated that claims 1-33 are rejected. By this communication, claims 1, 9, 13, 20, 26-27, and 33 are amended. Hence, claims 1-33 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

The Examiner objected to the disclosure because of the following informalities:

The Examiner noted the use of acronyms (i.e., IEEE, RSA, USB, etc.) throughout the specification without first including a description in plain text as required.

The disclosure was objected to because it contains an embedded hyperlink and/or other form of browser-executable code. The Examiner required Applicant to delete the embedded hyperlink and/or other form of browser-executable code per MPEP 608.01.

The Examiner also noted the use of the trademark Linux® in the application, and stated that it should be capitalized wherever it appears and be accompanied by the generic terminology. The Examiner further pointed out that although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Appropriate correction was required.

In reply, Applicant has amended the specification to first provide a description in plain text of all acronyms that are used. Applicant has in addition amended the specification to delete the embedded hyperlink and to capitalize "LINUX" and to accompany such use with generic terminology.

Accordingly, it is requested that the objections to the specification be withdrawn.

In addition, Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Claim Objections

The Examiner objected to claims 9 and 33 because the acronym "x86" is employed without first including a description in plain text as required.

In reply, Applicant respectfully traverses and notes that "x86" is not an acronym, but a well-known term of art that described a particular instruction set architecture that runs on x86-compatible microprocessors. However, in a good faith effort to further prosecution of this application through the Office, Applicant has amended claims 9 and 33 to recite "the instruction format for execution on an x86-compatible microprocessor" in place of "the x86 instruction format."

Consequently, it is requested that the objections to claims 9 and 33 be withdrawn.

Rejections Under 35 U.S.C. §112

The Examiner rejected claim 13 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner noted that it is unclear what "a number blocks" means, and stated that it appears that the applicant is attempting to claim, indicating "a number of blocks," and will interpret the claim in this manner.

In reply, Applicant asserts that the Examiner's interpretation of the claim is correct, and that claim 13 is amended by this communication to recite "a number of blocks." Accordingly, it is requested that the rejection of claim 13 be withdrawn

Rejections Under 35 U.S.C. §102(b)

The Examiner rejected claims 1-8, 10-12, 14-25, and 27-32 under 35 U.S.C. 102(e) as being anticipated by Yup et al. (US2002/0191784). Applicant respectfully traverses the Examiner's rejections.

As per claim 1, the Examiner noted that Yup et al. disclose an apparatus for performing cryptographic operations, comprising:

- a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes one of a plurality of cryptographic key sizes(AES block cipher can use varying key lengths) [page 4, paragraph 0045];
- and execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, said execution logic comprising: a key size controller (key expansion block), configured to employ said one of a plurality of cryptographic key sizes during execution of said one of the cryptographic operations [page 3, paragraph 0028].

In reply, Applicant respectfully disagrees with the Examiner's characterization of Yup vis-à-vis that subject matter which is recited in claim 1. To aid in the following analysis, claim 1, as amended herein, is repeated below.

1. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a microprocessor as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes one of a plurality of cryptographic key sizes; and

execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, said execution logic comprising:

a key size controller, configured to employ said one of a plurality of cryptographic key sizes during execution of said one of the cryptographic operations.

Applicant respectfully asserts that Yup et al. do no teach a cryptographic instruction. In fact, Applicant has been careful to search Yup et al. and reports that the term "cryptographic instruction" cannot be found. Yup et al. teach "A circuit includes a single circuit portion for implementing the Advanced Encryption Standard (AES) block cipher algorithm in a system having a plurality of channels. The circuit portion includes a circuit for individually generating, on the fly, the round keys used during each round of the AES block cipher algorithm. The circuit portion also includes shared logic circuits that implement the transformations used to encrypt and decrypt data blocks according to the AES block cipher. The single circuit portion encrypts or decrypts data blocks from each of the plurality of system channels in turn, in round-robin fashion. The circuit portion also includes a circuit for determining S-box values for the AES block cipher algorithm. The circuit additionally implements an efficient method for generating round keys on the fly for the AES block cipher decryption process. (Abstract)

It is unquestionable that Yup et al. teach a circuit for implementing the AES block cipher algorithm in a system having a plurality of channels. This is somewhat analogous to prior art stand-alone cryptographic processing units, the problems of which the present inventors have noted and for which the present invention is provided to overcome. Yup et al. is utterly silent with regard to how his invention is commanded to process data blocks other than to present a plurality of input registers 102 and associated control signals 103 that are coupled to a corresponding plurality of "system channels."

One skilled will appreciate that this type of configuration is cumbersome in that to provide for encryption and/or decryption of data, a processor must provide for communication with Yup et al.'s device via some system channel mechanism.

In stark contrast, claim 1 recites a cryptographic instruction that is received by a microprocessor as part of an instruction flow executing on said microprocessor. The claim continues to recited how the cryptographic instruction prescribes one of a plurality of key sizes. Yup et al. do not teach or suggest an instruction that provides for the foregoing limitation. The claim also recites execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations,

said execution logic comprising: a key size controller, configured to employ said one of a plurality of cryptographic key sizes during execution of said one of the cryptographic operations. Although Yup et al. teach a key expansion block, as the Examiner suggests, such a block is not operatively coupled to a cryptographic instruction, for Yup et al. is silent in this regard.

Based upon the above arguments, Applicant respectfully requests that the rejection of claim 1 be withdrawn.

With respect to claims 2-8, 10-12, and 14-19, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Yup et al. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-8, 10-12, and 14-19.

As per claim 20, the Examiner noted that Yup et al. disclose an apparatus for performing cryptographic operations, comprising:

- a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also prescribes a key size to be employed when executing said one of the cryptographic operations (AES block cipher can use varying key lengths) [page 4, paragraph 00451;
- and key size control logic(key expansion block), operatively coupled within said cryptography unit, configured to direct said device to employ said key size when performing said one of the cryptographic operations [page 3, paragraph 0028].

Applicant respectfully disagrees with the Examiner's arguments provided above and directs attention to the arguments submitted in traversal of the rejection of claim 1. In summary, Yup et al.'s invention is a stand-alone unit, not part of a microprocessor. As such, it does not execute an instruction flow. And furthermore, the instruction flow does not provide a cryptographic instruction that prescribes, *inter alia*, a key size to be employed when executing said one of the cryptographic operations.

In view of the above arguments, it is respectfully requested that the rejection of claim 20 be withdrawn.

With respect to claims 21-25, these claims depend from claim 20 and add further limitations that are neither anticipated nor made obvious by Yup et al. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 21-25.

As per claim 27, the Examiner noted that Yup et al. disclose a method for performing cryptographic operations in a device, the method comprising:

- receiving a cryptographic instruction that prescribes cryptographic key size for employment during execution of one of a plurality of cryptographic operations (AES block cipher can use varying key lengths) [page 4, paragraph 0045];
- and employing the cryptographic key size(key expansion block uses "nk", the key size, to generate a round key) when executing the one of the cryptographic operations [page 3, paragraphs 0028-00351.

Applicant respectfully disagrees with the points asserted above and directs the Examiner's attention to the arguments submitted in traversal of the rejections of claims 1 and 20. Claim 27 recites, among other elements and limitations, within a microprocessor, receiving a cryptographic instruction that prescribes cryptographic key size for employment during execution of one of a plurality of cryptographic operations. As noted earlier, Yup et al. does not teach a microprocessor, nor it is taught that the microprocessor receives a cryptographic instruction that prescribes cryptographic key size for employment during execution of one of a plurality of cryptographic operations. This is because Yup et al. teaches a stand-alone AES unit that is fed data from system channels.

Accordingly, it is respectfully requested that the rejection of claim 27 be withdrawn.

With respect to claims 28-32, these claims depend from claim 27 and add further limitations that are neither anticipated nor made obvious by Yup et al. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 28-32.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 9, 13, 26, and 33 under 35 U.S.C. 103(a) as being unpatentable over Yup et al.. Applicant respectfully traverses the Examiner's rejections and notes that claims 9, 13, 26, and 33 depend from claims 1, 20, and 27, as appropriate, and recited limitations above and beyond those elements which have been argued above as being allowable over the prior art of record. Consequently, Applicant respectfully requests that the Examiner withdraw the rejections of claims 9, 13, 26, and 33.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-33 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

08/03/2007

Date: _____